Journal of Number Theory **85**, 291–304 (2000)
doi:10.1006/jnth.2000.2547, available online at http://www.idealibrary.com on IDEAL®

A Two-Variable Artin Conjecture

Pieter Moree

KdV-Institute, University of Amsterdam, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands
E-mail: moree@wins.uva.nl

and

Peter Stevenhagen

Mathematisch Instituut, Universiteit Leiden, P.O. Box 9512, 2300 RA Leiden, The Netherlands
E-mail: psh@math.leidenuniv.nl

Communicated by P. Roquette

Received November 5, 1999

study the natural density $\delta(a, b)$ of the set of primes p for which the subgroup of $\mathbf{F}_p^*$ generated by $(a \bmod p)$ contains $(b \bmod p)$. It is shown that, under assumption of the generalized Riemann hypothesis, the density $\delta(a, b)$ exists and equals a positive rational multiple of the universal constant $S = \prod_{p \text{ prime}} (1 - p/(p^3 - 1))$. An explicit value of $\delta(a, b)$ is given under mild conditions on a and b. This extends and corrects earlier work of Stephens (1976, *J. Number Theory* **8**, 313–332). We also discuss the relevance of the result in the context of second order linear recurrent sequences and some numerical aspects of the determination of $\delta(a, b)$. © 2000 Academic Press

Key Words: Artin's conjecture; primitive roots; recurrence.

1. INTRODUCTION

Artin's original conjecture on primitive roots gives, for each non-zero integer a, a conjectural value $\delta(a)$ of the density of the set

$$\{p \text{ prime} : \langle a \bmod p \rangle = \mathbf{F}_p^*\} \tag{1.1}$$

inside the set of all primes. It equals $\delta(a) = c_a \cdot \prod_{p \text{ prime}} (1 - 1/p(p-1))$, where c_a is some explicit rational number that is positive whenever a is not equal to -1 or to a square. Artin's conjecture was proved by Hooley [3] under the assumption of the generalized Riemann hypothesis. Unconditionally, there is not a single value of a for which the set of primes in (1.1) has been proved to be infinite (cf. [9]).

In this paper we study the density $\delta(a, b)$ of the similarly defined set

$$\{p \text{ prime} : b \bmod p \in \langle a \bmod p \rangle \subset \mathbf{F}_p^*\} \tag{1.2}$$

inside the set of all primes. In view of our application in Section 6, we allow a and b to be nonzero *rational* numbers, and exclude the finitely

0022-314X/00 $35.00

many primes dividing the numerators and denominators of a and b from consideration in (1.2).

If a and b satisfy a multiplicative relation $a^x b^y = 1$ for exponents $x, y \in \mathbf{Z}$ that are not both equal to zero, then one can prove unconditionally that $\delta(a, b)$ is a rational number and that it is positive in all but a few trivial cases [14]. We will therefore restrict ourselves to the case where a and b are *multiplicatively independent* in $\mathbf{Q}^*$, i.e., no nontrivial relation of the type above holds. In this case, the following "two-variable Artin conjecture" has been proved unconditionally.

THEOREM 1. *Let $a, b \in \mathbf{Q}^*$ be multiplicatively independent. Then the set of primes defined by* (1.2) *is infinite.*

Theorem 1 is actually a special case of a theorem of Pólya [10], and we include its short and elementary proof in Section 6. It does not show that the set (1.2) contains a subset of primes of positive density.

We will mainly be concerned with the density of the set (1.2). Here the basic result is the following.

THEOREM 2. *Let $a, b \in \mathbf{Q}^*$ be multiplicatively independent, and assume the validity of the generalized Riemann hypothesis. Then $\delta(a, b)$ exists and equals*

$$\delta(a, b) = c_{a,b} \cdot \prod_{p \text{ prime}} \left(1 - \frac{p}{p^3 - 1}\right)$$

for some positive rational constant $c_{a,b}$.

The constant $c_{a,b}$ in the theorem depends on the degrees of the number fields

$$F_{i,j} = \mathbf{Q}(\zeta_{ij}, a^{1/ij}, b^{1/i}) \tag{1.3}$$

for $i, j \in \mathbf{Z}_{>0}$. Here ζ_{ij} denotes a primitive (ij)th root of unity. As an explicit formula for $c_{a,b}$ is rather cumbersome to write down, we only compute it explicitly in the "generic case" where the factor group $\mathbf{Q}^*/\langle -1, a, b\rangle$ is torsion-free. This means that $\pm a^x b^y$ is not an nth power in $\mathbf{Q}^*$ when x and y are not both divisible by n.

THEOREM 3. *Let $a, b \in \mathbf{Q}^*$ be multiplicatively independent, and suppose that the group $\mathbf{Q}^*/\langle -1, a, b\rangle$ is torsion-free. Define $r(n)$ for $n \in \mathbf{Z}_{\neq 0}$ by*

$$r(n) = \prod_{p \mid n \text{ prime}} \frac{-p^{4 - 3\,\mathrm{ord}_p(n)}}{p^3 - p - 1}.$$

Then the constant $c_{a,b}$ *in Theorem* 2 *has the value*

$$c_{a,b} = 1 + r(\mathrm{lcm}(2, \Delta(a))) + e(b)\, r(\Delta(b)) + e(ab)\, r(\Delta(ab)).$$

Here $\Delta(x) \in \mathbf{Z}$ *denotes the discriminant of the quadratic field* $\mathbf{Q}(\sqrt{x})$ *for* $x \in \mathbf{Q}^*$, *and we put*

$$e(x) = \begin{cases} \frac{3}{10} & \text{if } \Delta(x) \text{ is odd;} \\ 1 & \text{if } \Delta(x) \text{ is even.} \end{cases}$$

The universal constant $S = \prod_{p \text{ prime}} (1 - p/(p^3 - 1))$ in Theorem 2, which is the analogue of Artin's constant $A = \prod_{p \text{ prime}} (1 - 1/p(p-1))$ arising for the original Artin conjecture, already occurs in Stephens' paper [13]. Our Theorem 2 occurs for positive coprime integers a and b that are not perfect powers as [13, Theorem 3], but the explicit value for $c_{a,b}$ given there is involved and incorrect. The analytic part of Stephens' proof, which we summarize in the next section, is correct and generalizes in a rather straightforward way to our more general situation. His explicit evaluation of $c_{a,b}$, however, which is only carried through in one out of the eight subcases distinguished in [13], is incorrect, yielding an expression that is symmetric in a and b. Our proof of Theorem 3 separates the elementary calculus of double sums from the algebraic facts concerning the field degrees $[F_{i,j} : \mathbf{Q}]$.

In the final two sections we address the relevance of our results in the setting of second order recurrent sequences and deal with some numerical aspects of the density $\delta(a, b)$.

2. RESULTS OF HOOLEY AND STEPHENS

The proof of the special case of Theorem 2 occurring in [13] proceeds along the lines of Hooley's proof [3] of the original Artin conjecture.

Artin's basic observation is that, for $a \in \mathbf{Q}^*$ arbitrary and p a prime number with $\mathrm{ord}_p(a) = 0$, the index $[\mathbf{F}_p^* : \langle a \rangle]$ is divisible by j if and only if p splits completely in the splitting field $F_j = \mathbf{Q}(\zeta_j, a^{1/j})$ of the polynomial $X^j - a$ over $\mathbf{Q}$. By the Chebotarev density theorem, the set of these primes has natural density $1/[F_j : \mathbf{Q}]$. The primes p for which a is a primitive root modulo p are those primes that do *not* split completely in *any* of the fields F_j with $j > 1$. In fact, it suffices to require that p does not split completely in any field F_j with j *prime*. For Artin's conjecture, a standard inclusion–exclusion argument readily yields the heuristic value

$$\delta(a) = \sum_{j=1}^{\infty} \frac{\mu(j)}{[F_j : \mathbf{Q}]}. \tag{2.1}$$

The right-hand side of (2.1) converges whenever a is different from ± 1, since in that case $[F_j : \mathbf{Q}]$ differs from its "approximate value" $j \cdot \varphi(j)$, with φ denoting Euler's φ-function, by a factor that is easily bounded in terms of a. In fact, we obtain an upper bound for the upper density of the set (1.1) in this way. In order to turn this heuristic argument into a proof, Hooley employs estimates for the remainder term in the prime number theorem for the fields F_j that are currently only known to hold under assumption of the generalized Riemann hypothesis.

In the situation of Theorem 2, one can find a conjectural value for $\delta(a, b)$ in a similar way. For each integer $i \geqslant 1$, one considers the set of primes p with $\mathrm{ord}_p(a) = \mathrm{ord}_p(b) = 0$ for which the index $[\mathbf{F}_p^* : \langle a \rangle]$ is *equal* to i and the index $[\mathbf{F}_p^* : \langle b \rangle]$ is *divisible* by i. These are the primes that split completely in the field $F_{i,1} = \mathbf{Q}(\zeta_i, a^{1/i}, b^{1/i})$, but not in any of the fields $F_{i,j} = \mathbf{Q}(\zeta_{ij}, a^{1/ij}, b^{1/i})$ with $j > 1$. As before, inclusion–exclusion yields a conjectural value for the density $\delta_i(a, b)$ of this set of primes, and by summing over i we get

$$\delta(a, b) = \sum_{i=1}^{\infty} \delta_i(a, b) = \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} \frac{\mu(j)}{[F_{i,j} : \mathbf{Q}]}. \tag{2.2}$$

Note that $\delta_1(a, b)$ is nothing but the primitive root density $\delta(a)$ from (2.1).

As in the case of (2.1), the right-hand side of (2.2) converges if the degrees $[F_{i,j} : \mathbf{Q}]$ are not too far from their "approximate values" $i^2 j \cdot \varphi(ij)$. As we will see in Lemma 3.2, this is exactly what the hypothesis that a and b are multiplicativily independent implies.

The proof of (2.2) by Stephens [13], which assumes the Riemann hypothesis for each of the fields $F_{i,j}$, closely follows Hooley's argument in [3]. The restrictive hypotheses on integrality and coprimality of a and b are not in any way essential. The only requirement for the argument to work is that, up to a factor that can be uniformly bounded from below by some positive constant, $[F_{i,j} : \mathbf{Q}]$ behaves as $i^2 j \cdot \varphi(ij)$. We will show this in the next section, so there is no need for us to elaborate any further on the proof of (2.2); we will merely be dealing with degrees of radical extensions in order to prove Theorems 2 and 3.

The universal constant $S = \prod_{p \text{ prime}} (1 - p/(p^3 - 1))$ is the value of the right hand side of (2.2) obtained by substituting $[F_{i,j} : \mathbf{Q}] = i^2 j \cdot \varphi(ij)$, just like Artin's constant $A = \prod_{p \text{ prime}} (1 - 1/p(p-1))$ is obtained from the right hand side of (2.1) by putting $[F_j : \mathbf{Q}] = j \cdot \varphi(j)$. The "correction factors" c_a in Artin's conjecture and $c_{a,b}$ in Theorem 2 measure the deviation of the field degrees $[F_i : \mathbf{Q}]$ and $[F_{i,j} : \mathbf{Q}]$ from these values. As in the case of Artin's conjecture, the basic problem is that radical extensions of $\mathbf{Q}$ involving square roots are not in general linearly disjoint from cyclotomic extensions. In the case of Theorem 3, the situation is sufficiently simple to

allow an expression for $c_{a,b}$ by a formula that can be fitted on a single line. As the proof of Theorem 2 will show, all other cases can in principle be dealt with in a similar way.

For each prime q, the corresponding factor $1-1/q(q-1)$ in the definition of A has a well-known interpretation: it is, generically, the fraction of the primes p for which $\langle a \bmod p \rangle$ generates a subgroup of $\mathbf{F}_p^*$ of index not divisible by q. In a similar way, the factor $1-q/(q^3-1)$ at a prime q in the product for S represents, generically, the fraction of the primes p for which the number of factors q in the index $[\mathbf{F}_p^* : \langle a \bmod p \rangle]$ is *at most* the number of factors q in $[\mathbf{F}_p^* : \langle b \bmod p \rangle]$.

As in the case of Artin's conjecture, we cannot prove unconditionally that the set of primes in (1.2) has a positive lower density. The problem is that Chebotarev's density theorem only allows us to simultaneously impose conditions of the type above at primes q for *finitely many* primes q. As the fraction of primes that is eliminated by imposing a condition at q is generically positive, one can prove unconditionally that there exists a set of primes of positive density for which $b \bmod p$ is *not* contained in the subgroup $\langle a \bmod p \rangle$ of $\mathbf{F}_p^*$. This was already noted by Schinzel [12]. For the set (1.2) itself, the best unconditional result available is Theorem 1.

3. RADICAL EXTENSIONS

For Artin's original conjecture, one has to compute the degree of $F_j = \mathbf{Q}(\zeta_j, a^{1/j})$, the number field obtained by adjoining all j-th roots of an element $a \in \mathbf{Q}^* \setminus \{\pm 1\}$ to $\mathbf{Q}$. The result may be found in [15, Proposition 4.1]. The key observation is that if we take $a \neq \pm 1$ such that $\mathbf{Q}^*/\langle -1, a \rangle$ is torsion-free, then a is a square in $\mathbf{Q}(\zeta_n)$ if and only if the discriminant $\Delta(a)$ of $\mathbf{Q}(\sqrt{a})$ divides n; moreover, a is not a kth power with $k>2$ in any cyclotomic extension of $\mathbf{Q}$. If j_1 divides j and a is as above, then Kummer theory yields

$$[\mathbf{Q}(\zeta_j, a^{1/j_1}) : \mathbf{Q}] = \begin{cases} \frac{1}{2} j_1 \cdot \varphi(j) & \text{if 2 divides } j_1 \text{ and } \Delta(a) \text{ divides } j, \\ j_1 \cdot \varphi(j) & \text{otherwise.} \end{cases} \tag{3.1}$$

For arbitrary $a \in \mathbf{Q}^* \setminus \{\pm 1\}$ and $j \in \mathbf{Z}_{>0}$, let $t = \gcd\{\operatorname{ord}_p(a) : p \text{ prime}\}$ be the order of the torsion subgroup of $\mathbf{Q}^*/\langle -1, a \rangle$, and take $j_1 = j/\gcd(j, t)$. There are two cases. If a is a tth power in $\mathbf{Q}^*$, say $a = a_1^t$, we have $F_j = \mathbf{Q}(\zeta_j, a^{1/j}) = \mathbf{Q}(\zeta_j, a_1^{1/j_1})$ and (3.1) can be applied directly. If a is not a tth power, then t is even and $-a = a_1^t$ is a tth power in $\mathbf{Q}^*$. We have an extension

$$\mathbf{Q}(\zeta_j, \zeta_{2j} a_1^{1/j_1}) = F_j \subset F_j' = \mathbf{Q}(\zeta_{2j}, a_1^{1/j_1})$$

of F_j of degree at most 2 for which the degree $[F'_j : \mathbf{Q}]$ is given by (3.1), and one is left with the determination of $[F'_j : F_j] \in \{1, 2\}$ as in [15]. A somewhat subtle case distinction is necessitated by the peculiarity that the element -4, which is not a square in $\mathbf{Q}^*$, turns out to be equal to $(1+\zeta_4)^4$ in $\mathbf{Q}(\zeta_4)$. Note that if we have $[F'_j : F_j] = 2$, then j and t are even and $2j_1$ divides j. Thus, the "degree loss" $j\varphi(j)/[F_j : \mathbf{Q}]$ with respect to the generic value $j\varphi(j)$ is always an integer dividing $2t$. The factor 2 reflects the fact the kernel of the natural map

$$\mathbf{Q}^*/\mathbf{Q}^{*k} \to \mathbf{Q}(\zeta_k)^*/\mathbf{Q}(\zeta_k)^{*k}$$

is an abelian group annihilated by 2. More precisely, it vanishes if k is odd; if k is even it is generated by the elements $x^{k/2}\mathbf{Q}^{*k}$ satisfying $\Delta(x) \mid k$ and, for $k \equiv 4 \bmod 8$, the element $-2^{k/2}\mathbf{Q}^{*k}$.

In our two-variable setting, where we deal with the fields $F_{i,j} = \mathbf{Q}(\zeta_{ij}, a^{1/ij}, b^{1/i})$, the statement in terms of the map above easily leads to the following generalization.

PROPOSITION 3.2. *Let $a, b \in \mathbf{Q}^*$ be multiplicatively independent, and let t be the order of the torsion subgroup of $\mathbf{Q}^*/\langle -1, a, b\rangle$. Then for all $i, j \in \mathbf{Z}_{>0}$, the quantity*

$$f_{i,j} = \frac{i^2 j\varphi(ij)}{[\mathbf{Q}(\zeta_{ij}, a^{1/ij}, b^{1/i}) : \mathbf{Q}]}$$

is a positive integer dividing $4t$. In the torsionfree case $t = 1$, it is equal to

the number of elements in $\{1, \Delta(a), \Delta(b), \Delta(ab)\}$ dividing ij if i is even;

the number of elements in $\{1, \operatorname{lcm}(2, \Delta(a))\}$ dividing ij if i is odd.

Proof. Pick $i, j \in \mathbf{Z}_{>0}$ and write $k = ij$. Let $W_{i,j} \subset \mathbf{Q}^*$ be the subgroup generated by a and $b^j = b^{k/i}$, and $\bar{W}_{i,j}$ the image of $W_{i,j}$ in $\mathbf{Q}^*/\mathbf{Q}^{*k}$. As the order of $\bar{W}_{i,j}$ divides $ik = i^2 j$, we write $i^2 j = \#\bar{W}_{i,j} \cdot t_{i,j}$ with $t_{i,j} \in \mathbf{Z}_{>0}$. By Kummer theory, the degree of

$$F_{i,j} = \mathbf{Q}(\zeta_{ij}, a^{1/ij}, b^{1/i}) = \mathbf{Q}(\zeta_k, \sqrt[k]{W_{i,j}})$$

over $\mathbf{Q}(\zeta_k)$ equals $\#\psi[\bar{W}_{i,j}]$, with $\psi: \bar{W}_{i,j} \to \mathbf{Q}(\zeta_k)^*/\mathbf{Q}(\zeta_k)^{*k}$ the natural map. We deduce that the "degree loss" $f_{i,j}$ for $F_{i,j}$ can be written as $f_{i,j} = t_{i,j} \cdot \#\ker\psi$. It is a decomposition of $f_{i,j}$ into a factor $t_{i,j}$ coming from "torsion in $\mathbf{Q}^*$" and a factor $\#\ker\psi$ measuring the additional torsion caused by the adjunction of ζ_k.

As $\bar{W}_{i,j}$ is a finite abelian group on 2 generators and $\ker\psi \subset \bar{W}_{i,j}$ is annihilated by 2, it is clear that $\#\ker\psi$ divides 4. In order to show that $t_{i,j}$ divides t, we let $T \subset \mathbf{Q}^*$ be the inverse image of the torsion subgroup

of $\mathbf{Q}^*/\langle -1, a, b\rangle$ under the natural map $\mathbf{Q}^* \to \mathbf{Q}^*/\langle -1, a, b\rangle$. Then T contains $V = \langle -1, a, b\rangle$ as a subgroup of index t, and $\bar{W}_{i,j}$ is the subgroup of $T/T^k \subset \mathbf{Q}^*/\mathbf{Q}^{*k}$ generated by a and $b^j = b^{k/i}$. The integer $t_{i,j}$ is the order of the kernel of the composed map

$$\frac{\langle a, b^j\rangle}{\langle a^k, b^k\rangle} = \frac{W_{i,j}}{W_{i,j} \cap V^k} \to V/V^k \to T/T^k,$$

so it divides $\#\ker[V/V^k \to T/T^k]$. As V/V^k and T/T^k are finite abelian groups of the same order, $\#\ker f = \#\operatorname{coker} f = [T: VT^k]$ divides $[T: V] = t$. This shows that $f_{i,j}$ divides $4t$.

Assume now that $\mathbf{Q}^*/\langle -1, a, b\rangle$ is torsion-free. Then we have $T = V$ and $t_{i,j} = 1$ in the argument above, and $f_{i,j} = \#\ker\psi$. Clearly, $\ker\psi$ vanishes if k is odd. If k is even, the 2-torsion subgroup of $\bar{W}_{i,j}$ is generated by $a^{k/2}$ if i is odd and by $a^{k/2}$ and $b^{k/2}$ if i is even. As ψ vanishes on the residue class of $x^{k/2} \in \langle a^{k/2}, b^{k/2}\rangle$ in $\bar{W}_{i,j}$ if and only if $\Delta(x)$ divides k, we arrive at the value for $t_{i,j}$ given in the lemma. ∎

COROLLARY 3.3. *The integer $f_{i,j}$ in Proposition* 3.2 *only depends on the greatest common divisors* $\gcd(i, 2t)$ *and* $\gcd(ij, 8st)$, *where s is the product of the primes p for which* $\operatorname{ord}_p(a)$ *and* $\operatorname{ord}_p(b)$ *are not both equal to* 0.

Proof. In the proof above, one needs $\gcd(k, t) = \gcd(ij, t)$ to determine the kernel $\ker[V/V^k \to T/T^k]$ and $\gcd(i, t)$ to determine the order $t_{i,j}$ of the intersection of $W_{i,j} = \langle a, b^{k/i}\rangle$ with this kernel. As $\Delta(x)$ divides $4s$ for all $x \in V$, we can determine the kernel of $V/V^k \to \mathbf{Q}(\zeta_k)^*/\mathbf{Q}(\zeta_k)^{*k}$ if we know $\gcd(k, 8s) = \gcd(ij, 8s)$. Knowledge of the parity of i enables us to intersect this kernel with $W_{i,j}/(W_{i,j} \cap V^k)$, thus yielding the second factor $\#\ker\psi$ in $t_{i,j}$. ∎

4. EVALUATION OF THE BASIC DOUBLE SUM

From (2.2), Proposition 3.2, and Corollary 3.3 it is clear that, in order to evaluate $\delta(a, b)$, we need to evaluate for nonzero integers m, n the double sum

$$S_{m,n} = \sum_{\substack{i=1 \\ m \mid i}}^{\infty} \sum_{\substack{j=1 \\ mn \mid ij}}^{\infty} \frac{\mu(j)}{i^2 j \varphi(ij)}. \tag{4.1}$$

This is a rather straightforward computation in elementary number theory leading to the following result.

THEOREM 4.2. *For $m, n \in \mathbf{Z}_{>0}$, the value $S_{m,n}$ of the series in* (4.1) *is the rational multiple*

$$S_{m,n} = \frac{S}{m^3 n^3} \prod_{p \mid n} \frac{-p^4}{p^3 - p - 1} \prod_{\substack{p \mid m \\ p \nmid n}} \frac{p^3 + p^2}{p^3 - p - 1}$$

of the universal constant $S = \prod_{p \text{ prime}} (1 - \frac{p}{p^3 - 1})$ occurring in Theorem 2.

Proof. We can sum over all $i \geqslant 1$ in (4.1) after substituting mi for i. Putting $ij = nd$ and summing over all $d \geqslant 1$ then yields

$$S_{m,n} = \frac{1}{m^2 n^2} \sum_{d=1}^{\infty} \frac{1}{d^2 \varphi(mnd)} \sum_{j \mid nd} j\mu(j).$$

Writing $\tilde{x} = \prod_{p \mid x} p$ for the largest squarefree divisor of x, we have for any integer x

$$\sum_{j \mid x} j\mu(j) = \sum_{j \mid \tilde{x}} j\mu(j) = \mu(\tilde{x}) \sum_{j \mid \tilde{x}} j\mu(\tilde{x}/j) = \mu(\tilde{x})\, \varphi(\tilde{x}).$$

This enables us to write

$$S_{m,n} = \frac{1}{m^2 n^2} \sum_{d=1}^{\infty} \frac{\mu(\widetilde{nd})\, \varphi(\widetilde{nd})}{d^2 \varphi(mnd)} = \frac{\mu(\tilde{n})\, \varphi(\tilde{n})}{m^2 n^2 \varphi(mn)} \sum_{d=1}^{\infty} f(d),$$

where f is the *multiplicative* function defined by

$$f(d) = \frac{1}{d^2} \cdot \frac{\varphi(mn)}{\varphi(mnd)} \cdot \frac{\mu(\widetilde{nd})}{\mu(\tilde{n})} \cdot \frac{\varphi(\widetilde{nd})}{\varphi(\tilde{n})}.$$

As $\sum_{d=1}^{\infty} f(d)$ is absolutely convergent, we can use the values

$$f(p^k) = \begin{cases} -p^{1-3k}, & \text{for } p \nmid mn; \\ p^{-3k}, & \text{for } p \mid n; \\ -(p-1)\, p^{-3k}, & \text{for } p \mid m,\ p \nmid n, \end{cases}$$

of f on the prime powers p^k with $k \geqslant 1$ to obtain an Euler product expansion

$$S_{m,n} = \frac{\mu(\tilde{n})\,\varphi(\tilde{n})}{m^2 n^2 \varphi(mn)} \prod_{p \mid n} \frac{p^3}{p^3-1} \prod_{p \mid m,\ p \nmid n} \frac{p^3-p}{p^3-1} \prod_{p \nmid mn} \frac{p^3-p-1}{p^3-1}$$
$$= \frac{S}{m^3 n^3} \frac{mn}{\phi(mn)} \prod_{p \mid n} \frac{(1-p)\,p^3}{p^3-p-1} \prod_{p \mid m,\ p \nmid n} \frac{p^3-p}{p^3-p-1}$$
$$= \frac{S}{m^3 n^3} \prod_{p \mid n} \frac{-p^4}{p^3-p-1} \prod_{p \mid m,\ p \nmid n} \frac{p^3+p^2}{p^3-p-1}. \quad \blacksquare$$

COROLLARY 4.3. *Define $r(n)$ as in Theorem 3. Then we have $S_{1,n} = r(n)\,S$ and*

$$S'_{2,n} := \sum_{\substack{i=1 \\ 2 \mid i}}^{\infty} \sum_{\substack{j=1 \\ n \mid ij}}^{\infty} \frac{\mu(j)}{i^2 j \varphi(ij)} = \begin{cases} \frac{3}{10} r(n)\,S & \text{if } n \text{ is odd;} \\ r(n)\,S & \text{if } 4 \mid n. \end{cases}$$

Proof. The first equality is immediate by taking $m = 1$ in 4.2.

If n is odd, we have $S'_{2,n} = S_{2,n} = (3/10)\,r(n)\,S$. If 4 divides n, the condition $2 \mid i$ in the definition of $S'_{2,n}$ is superfluous as $\mu(j)$ vanishes for $4 \mid j$. It therefore equals $S'_{2,n} = S_{1,n} = r(n)\,S$. $\blacksquare$

5. PROOF OF THEOREMS 2 AND 3

We now have everything at our disposal to prove Theorems 2 and 3.

Proof of Theorem 2. We substitute the value of $[F_{i,j} : \mathbf{Q}]$ from Lemma 3.2 into the expression for $\delta(a, b)$ provided by (2.2) to obtain

$$\delta(a, b) = \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} f_{i,j} \frac{\mu(j)}{i^2 j \varphi(ij)}. \tag{5.1}$$

By Proposition 3.2, there are only finitely many values of $f_{i,j}$ that can occur, namely the divisors of $4t$. By Corollary 3.3, the value of $f_{i,j}$ only depends on the greatest common divisors of i and ij with certain integers depending on a and b. It follows that the set of pairs (i, j) for which $f_{i,j}$ equals a given divisor of $4t$ can be characterized in terms of a finite number of divisibility criteria on i and ij. This enables us to write $\delta(a, b)$ as an integral linear combination of our basic sums $S_{m,n}$ for suitable values of m and n. As each of these sums is a rational multiple of S by 4.2, we conclude that $\delta(a, b)$ is itself a rational multiple of S.

It is not at all clear from the preceding argument that the resulting value for $\delta(a, b)$ will always be positive. From the expression $\delta(a, b) = \sum_{i=1}^{\infty} \delta_i(a, b)$ as a sum of nonnegative terms in (2.2), we see that it suffices to

show that there is a value of i for which $\delta_i(a, b)$ is nonzero. If a is not a square we can take $i=1$ as $\delta_1(a, b)=\delta(a)$ is then positive by Hooley's result. For arbitrary a, there can be many values of i with $\delta_i(a, b)=0$. In fact, for many i one can construct a that satisfy $[\mathbf{F}_p^*: \langle a \rangle] \neq i$ for almost all p. A list of such values of i can be found in [5, (8.9)–(8.13)]. The smallest value that is not in the list is $i=24$, and we will show that not only $\delta_{24}(a)$, but also $\delta_{24}(a, b)$, is always positive.

We are interested in the primes p for which $[\mathbf{F}_p: \langle a \rangle]$ equals 24 and $[\mathbf{F}_p: \langle b \rangle]$ is divisible by 24. Up to finitely many exceptions these are the primes that split completely in the field $E=\mathbf{Q}(\zeta_{24}, \sqrt[24]{a}, \sqrt[24]{b})$, but not in any of its extensions $E_n=\mathbf{Q}(\zeta_{24n}, \sqrt[24n]{a}, \sqrt[24]{b})$ for $n>1$. By the results of Lenstra [5, Theorem 4.1], the set of these primes has positive density (under GRH) unless there is an obstruction "at a finite level," i.e., an integer h such that every automorphism σ of the extension $E \subset E_h$ is trivial on $E_{n(\sigma)}$ for some divisor $n(\sigma)>1$ of h. Thus, it suffices to show that for each square-free integer h, there exists $\sigma \in \mathrm{Gal}(E_h/\mathbf{Q})$ satisfying the following two conditions:

1. σ is the identity on E;

2. if p is a prime dividing h and q is the largest power of p dividing $24h$, then σ is not the identity on $\mathbf{Q}(\zeta_q)$.

In order to construct such an automorphism, we observe that the maximal subfield $E^{\mathrm{ab}} \subset E$ that is abelian over $\mathbf{Q}$ has the property that $\mathrm{Gal}(E^{\mathrm{ab}}/\mathbf{Q})$ is an elementary abelian 2-group. Assume without loss of generality that 6 divides h, and let q be a prime power as in Condition 2. Take σ_q to be any nontrivial automorphism of $\mathbf{Q}(\zeta_q)$ that is a *square* in $\mathrm{Gal}(\mathbf{Q}(\zeta_q)/\mathbf{Q})$. As q is not a divisor of 24, the group $\mathrm{Gal}(\mathbf{Q}(\zeta_q)/\mathbf{Q}) \cong (\mathbf{Z}/q\mathbf{Z})^*$ is not of exponent 2, and such an element σ_q exists. Define σ_0 as the automorphism of $\mathbf{Q}(\zeta_{24h})$ with restrictions $\sigma|_{\mathbf{Q}(\zeta_q)}=\sigma_q$. Then σ_0 is a square in $\mathrm{Gal}(\mathbf{Q}(\zeta_{24h})/\mathbf{Q})$, so it is the identity on $E \cap \mathbf{Q}(\zeta_{24h}) \subset E^{\mathrm{ab}}$. This implies that there is a unique extension of σ_0 to $E(\zeta_{24h})$ that is the identity on E. Any extension σ of this automorphism of $E(\zeta_{24h})$ to E_h now meets our requirements. ∎

Proof of Theorem 3. In the case where $a, b \in \mathbf{Q}^*$ are multiplicatively independent and $\mathbf{Q}^*/\langle -1, a, b \rangle$ is torsion-free, we can use the values of $f_{i,j}$ from Lemma 3.2 and rewrite (5.1) explicitly as an integral linear combination of the type encountered in the proof of Theorem 2. The sums of the type $S'_{2,n}$ from 4.3, which single out the contribution to $S_{1,n}$ of the terms with even i, can be used to obtain the compact expression

$$\delta(a, b)=S_{1,1}+S'_{2,\Delta(a)}+S'_{2,\Delta(b)}+S'_{2,\Delta(ab)}+(S_{1,\mathrm{lcm}(2,\Delta(a))}-S'_{2,\mathrm{lcm}(2,\Delta(a))}).$$

The sum of the three terms involving $\Delta(a)$ yields $S_{1,\,\mathrm{lcm}(2,\,\Delta(a))}$, since we have $S'_{2,\,\Delta(a)} = S'_{2,\,\mathrm{lcm}(2,\,\Delta(a))}$; this is immediate if $\Delta(a)$ is even, and if $\Delta(a)$ is odd the equality $S'_{2,\,\Delta(a)} = S'_{2,\,2\Delta(a)}$ follows directly from the definition of the sum $S'_{2,\,n}$ in 4.3. The explicit value of $c_{a,\,b} = \delta(a, b)/S$ now follows easily from the two statements in 4.3. ∎

6. REFORMULATION IN TERMS OF RECURRENT SEQUENCES

If we write the rational numbers a and b in Theorems 2 and 3 as $a = a_1/a_2$ and $b = b_1/b_2$, then we find that the set of primes that divide some term of the integer sequence $\{b_2 a_1^n - b_1 a_2^n\}_{n=0}^{\infty}$ has positive density. This formulation in terms of integers is useful in proving the unconditional result in Theorem 1. The proof given below, which is entirely elementary, is an easy extension of the argument of Pólya occurring in [11, Chap. 8, Problem 107]. A generalization to integer sequences of the form $\{\sum_{i=1}^{k} c_i a_i^n\}_{n=0}^{\infty}$ for arbitrary $k \geqslant 2$ was given by Pólya in [10].

Proof of Theorem 1. Write $a = a_1/a_2$ and $b = b_1/b_2$ as above and take $\gcd(a_1, a_2) = \gcd(b_1, b_2) = 1$. We have $a_1 \neq \pm a_2$ by the hypothesis that $a, b \in \mathbf{Q}^*$ are multiplicativily independent, so $|x_n|$ tends to infinity with n. We need to show that the set S of primes that divide $x_n = b_2 a_1^n - b_1 a_2^n$ for some $n \geqslant 0$ is infinite.

Suppose that S is finite, and set $\ell = \varphi(|x_0| \cdot \prod_{p \in S} p)$. Clearly, we have $\ell > 0$. We derive a contradiction by showing that the sequence $\{x_{\ell n}\}_{n=0}^{\infty}$ is bounded. As S is finite, it suffices to show that $\mathrm{ord}_p(x_{\ell n})$ remains bounded as a function of n for each $p \in S$. Suppose that $p \in S$ is a prime that does *not* divide $a_1 a_2$. Then we have $\mathrm{ord}_p(x_{\ell n}) = \mathrm{ord}_p(x_0)$ for all n since

$$x_{\ell n} - x_0 = b_2(a_1^{\ell n} - 1) - b_1(a_2^{\ell n} - 1)$$

is by the definition of ℓ divisible by $p^{\mathrm{ord}_p(x_0)+1}$. Suppose that $p \in S$ is a prime dividing $a_1 a_2$. Then p divides exactly one of a_1 and a_2, say a_1, and we have $\mathrm{ord}_p(x_{\ell n}) = \mathrm{ord}_p(b_1)$ for all sufficiently large n. ∎

Integer sequences of the form $\{b_2 a_1^n - b_1 a_2^n\}_{n=0}^{\infty}$ are linear recurrent sequences of order 2. They can be defined by the recursion $x_{k+2} = (a_1 + a_2) x_{k+1} - a_1 a_2 x_k$ for all $k \geqslant 0$ and the initial values $x_0 = b_2 - b_1$ and $x_1 = b_2 a_1 - b_1 a_2$.

Much effort has been spent on the determination of the set of primes dividing linear recurrent integer sequences; see [2] and the references given there. In the case of second order sequences, our Theorems 1–3 lead to the following result.

THEOREM 4. *Let $r, s \in \mathbf{Q}$ be rational numbers and $\mathscr{R} = \{x_n\}_{n=0}^{\infty}$ an integer sequence satisfying the second order recursion $x_{k+2} = rx_{k+1} - sx_k$ for all $k \geqslant 0$. Suppose that $X^2 - rX + s$ splits in $\mathbf{Q}[X]$ and that $\mathscr{R}$ does not satisfy a first order recursion. Then the set of primes that divide some term of $\mathscr{R}$ is infinite; if we assume the generalized Riemann hypothesis, it has positive density.*

Proof. Let $a_1, a_2 \in \mathbf{Q}$ be the two roots of the polynomial $X^2 - rX + s$.

Suppose first that we have $a_1 \neq a_2$. Then we have $x_n = b_2 a_1^n - b_1 a_2^n$ for certain $b_1, b_2 \in \mathbf{Q}$. As X does not satisfy a first order recurrence, we have $a_1 a_2 \neq 0$ and $b_1 b_2 \neq 0$. After replacing, if necessary, the sequence $\{x_n\}_{n=0}^{\infty}$ by $\{\lambda^n x_n\}_{n=0}^{\infty}$ for suitable $\lambda \in \mathbf{Q}^*$, we may assume that a_1 and a_2 are coprime integers. This only changes the set of primes that divide some term of $\mathscr{R}$ by finitely many primes. In a similar way, after replacing $\{x_n\}_{n=0}^{\infty}$ by $\{\lambda x_n\}_{n=0}^{\infty}$ for suitable $\lambda \in \mathbf{Q}^*$, we may assume that b_1 and b_2 are coprime integers. If $a = a_1/a_2$ and $b = b_1/b_2$ are multiplicativily independent in $\mathbf{Q}^*$, we are in the situation of Theorems 1 and 2, and we are done. If a and b are multiplicativily dependent, then the results on torsion sequences from [14] imply unconditionally that the set of primes that divide some term of $\mathscr{R}$ has positive density.

Suppose next that we are in the inseparable case $a_1 = a_2$. Then we have $x_n = (b_1 + b_2 n)\, a_1^n$, for certain $b_1, b_2 \in \mathbf{Q}$, and $b_2 \neq 0$ by assumption. Now all primes that do not divide b_2 divide some term of $\mathscr{R}$, so we obtain a set of prime divisors of density 1. ∎

The hypothesis that $\mathscr{R}$ does not satisfy a first order recursion in Theorem 4 is only there to exclude trivialities. In order to remove the assumption that $X^2 - rX + s$ splits in $\mathbf{Q}[X]$, one needs to prove the analogues of our Theorems 1 and 2 for the set (1.2) in the case where a and b are elements of norm 1 in a quadratic number field K and $\mathbf{F}_p$ is replaced by the ring of integers of K modulo the principal ideal (p). It turns out that the inert primes lead to various complications. The torsion case can be found in [14] and, for the special case where a comes from the fundamental unit of K, in [7]. For a treatment of the nontorsion example proposed by Lagarias [4, p. 451], we refer the reader to [8].

7. NUMERICAL DATA

Just like Artin's constant $A = \prod_{p \text{ prime}} (1 - 1/p(p-1))$, the universal constant $S = \prod_{p \text{ prime}} (1 - p/(p^3 - 1))$ in Theorem 2 is defined by a slowly converging product. One can obtain good numerical approximations to S, such as the approximation

$$S \approx 0.57595\ 99688\ 92945\ 43964\ 31633\ 75492\ 49669\ 25065\ 13967\ 17649$$

up to 50 decimal digits, by expressing $-\log S$ as a rapidly converging series involving the values $\zeta(d)$ of the Riemann zeta function at arguments $d \geqslant 2$. This is done for Artin's constant in [1], and for S the expression

$$-\log S = -\log \zeta(3) + \sum_{d=2}^{\infty} \sum_{k \mid d} \log \zeta(d) \frac{a_k}{d} \mu\left(\frac{d}{k}\right)$$

is derived in [6]. Here a_k is defined by its initial values $a_1 = 0$, $a_2 = 2$, $a_3 = 3$, and the recursion formula $a_{k+3} = a_{k+1} + a_k$ for $k \geqslant 1$.

It is not computationally feasible to determine the rational numbers $c_{a,b}$ in Theorem 2 from numerical data. In the torsionfree case occurring in Theorem 3, the value of $c_{a,b}$ lies between the extremal values

$$c_{\min} = c_{2,5} = \frac{9343}{9520} \approx .981 \qquad \text{and} \qquad c_{\max} = c_{5,3} = \frac{28001}{27370} \approx 1.023.$$

For the 41,535 primes contained in the interval [7, 500 000], one finds that we have $\bar{5} \in \langle 2 \bmod p \rangle$ for 23,498 primes and $\bar{3} \in \langle 5 \bmod p \rangle$ for 24,429 primes. When divided by S, these fractions are approximately equal to 0.9823 and 1.0212, respectively. This shows that the deviations from S are "numerically visible" in a qualitative sense, but it also makes clear that one cannot determine the fraction $c_{a,b}$ from such data.

REFERENCES

1. E. Bach, The complexity of number theoretic constants, *Inform. Process. Lett.* **62** (1997), 145–152.
2. C. Ballot, Density of prime divisors of linear recurrent sequences, *Mem. Amer. Math. Soc.* **551** (1995).
3. C. Hooley, On Artin's conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.
4. J. C. Lagarias, The set of primes dividing the Lucas numbers has density 2/3, *Pacific J. Math.* **118** (1985), 449–461; Erratum, *Pacific J. Math.* **162** (1994), 393–397.
5. H. W. Lenstra, Jr, On Artin's conjecture and Euclid's algorithm in global fields, *Invent. Math.* **42** (1977), 201–224.
6. P. Moree, Approximation of singular series and automata, *Manuscripta Math.* **101** (2000), 385–399.
7. P. Moree and P. Stevenhagen, Prime divisors of Lucas sequences, *Acta Arith.* **82**, No. 4 (1997), 403–410.
8. P. Moree and P. Stevenhagen, Prime divisors of the Lagarias sequence, *J. Théor. Nombres Bordeaux*, to appear.
9. M. Ram Murty, Artin's conjecture for primitive roots, *Math. Intelligencer* **10**, No. 4 (1988), 59–67.
10. G. Pólya, Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen, *J. Reine Angew. Math.* **151** (1921), 1–31.
11. G. Pólya and G. Szegö, "Aufgaben und Lehrsätze aus der Analysis," Springer, Berlin, 1925.

12. A. Schinzel, On the congruence $a^x \equiv b \pmod{p}$, *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astron. Phys.* **8** (1960), 307–309.
13. P. J. Stephens, Prime divisors of second order linear recurrences, *J. Number Theory* **8** (1976), 313–332.
14. P. Stevenhagen, Prime densities for second order torsion sequences, preprint, 2000.
15. S. S. Wagstaff, Pseudoprimes and a generalization of Artin's conjecture, *Acta Arith.* **41** (1982), 141–150.